GroupWise® Mobility Service 18
Installation Guide

March 2018

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.novell.com/company/legal/.

Copyright © 2017 Micro Focus Software Inc. All Rights Reserved.

Contents

About This Guide **5**

1 GroupWise Mobility Service Product Overview **7**

Mobility Server Configuration . . . 7
Single Mobility Server System . . . 8
Multiple Mobility Server System . . . 8
Synchronization Capabilities . . . 9

2 GroupWise Mobility Service System Requirements **11**

Mobility Server Requirements . . . 11
Directory Requirements . . . 12
Web Browser Requirements for the Mobility Admin Console . . . 12
GroupWise Requirements . . . 12
Mobile Device Requirements . . . 13
Recommended Number of Devices . . . 14

3 GroupWise Mobility Service Installation **17**

Planning a Mobility System . . . 17
- Planning the Configuration of Your Mobility System . . . 17
- Selecting Mobility Servers . . . 18
- Selecting the User Source for Your Mobility System . . . 18
- Gathering LDAP Information (Optional) . . . 19
- Gathering GroupWise System Information . . . 21
- Gathering Mobile Device Information . . . 23
- Planning the Mobility Database . . . 25
- Establishing Mobility System Security . . . 25

Preparing to Install the Mobility Service . . . 26
- Preparing the Linux Server . . . 26
- Opening Required Ports . . . 27
- Verifying GroupWise System Availability . . . 27
- Verifying Certificate Availability . . . 28

Installing the Mobility Service . . . 28
- Obtaining the GroupWise Mobility Service 18 ISO . . . 28
- Running the Mobility Service Installation Program . . . 29
- Checking the Status of the Mobility Service . . . 30
- Using the Mobility Admin Console . . . 30
- Uninstalling the Mobility Service . . . 31

Adding Users to Your Initial Mobility System . . . 32

Testing Your Initial Mobility System . . . 33
- Managing Initial Synchronization of Users . . . 33
- Helping Mobile Device Users Understand Synchronization . . . 34
- Testing Synchronization . . . 34

Integrating with Mobile Device Management Applications . . . 35
- Micro Focus ZENworks Mobile Management . . . 35
- Other MDM Solutions . . . 37

What's Next . . . 37
- Managing Your Mobility System . . . 37
- Managing the GroupWise Sync Agent . . . 38

Managing the Device Sync Agent 38
GroupWise Mobility Service Installation Worksheet 38

4 GroupWise Mobility Service Update 41

Updating to GroupWise Mobility Service 18 41
Obtaining the GroupWise Mobility Service 18 ISO 41
Upgrading GroupWise Mobility Service 42
Checking the Status of the Mobility Service after Update 43
Changing the User Source for Your Mobility System (Optional). 43

A GroupWise Mobility Service Installation Troubleshooting 45

About This Guide

The *GroupWise Mobility Service 18 Installation Guide* helps you to understand and set up a GroupWise Mobility system by installing the GroupWise Mobility Service, which includes the GroupWise Sync Agent and the Mobility Sync Agent.

- Chapter 1, "GroupWise Mobility Service Product Overview," on page 7
- Chapter 2, "GroupWise Mobility Service System Requirements," on page 11
- Chapter 3, "GroupWise Mobility Service Installation," on page 17
- Chapter 4, "GroupWise Mobility Service Update," on page 41
- Appendix A, "GroupWise Mobility Service Installation Troubleshooting," on page 45

Audience

This guide is intended for network administrators who install a Mobility system to provide data synchronization between GroupWise and mobile devices.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation.

Additional Documentation

For all GroupWise Mobility Service documentation, see the GroupWise Mobility Service 18 Documentation website (http://www.novell.com/documentation/groupwise18).

- GroupWise Mobility Quick Start for Mobile Device Users
- GroupWise Mobility Service 18 Readme
- GroupWise Mobility Service 18 Administration Guide

In addition to the GroupWise Mobility Service product documentation, the following resources provide information about the Mobility Service:

- Novell Support and Knowledgebase (http://www.novell.com/support)
- GroupWise Mobility Service Cool Solutions (https://www.novell.com/communities/coolsolutions/tag/groupwise-mobility-service)
- GroupWise Mobility Service Devices Wiki (http://wiki.novell.com/index.php/GroupWise_Mobility_Devices)
- GroupWise Support Forums (https://forums.novell.com/forumdisplay.php/1297-GroupWise)
- GroupWise Product Website (http://www.novell.com/products/groupwise)

1 GroupWise Mobility Service Product Overview

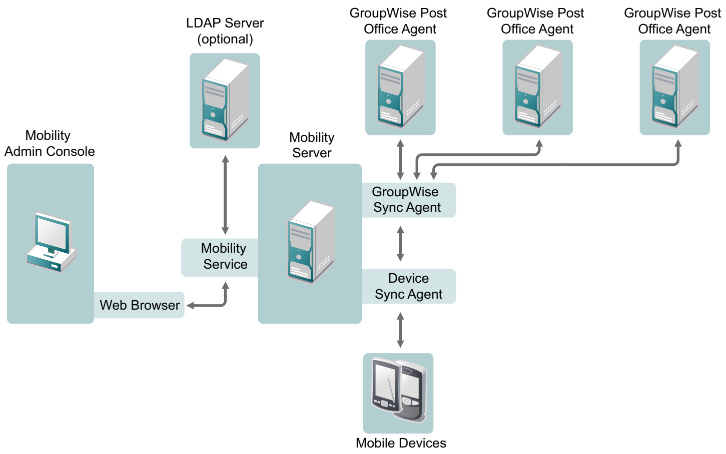
The GroupWise Mobility Service provides data synchronization between GroupWise mailboxes and mobile devices for synchronizing email, appointments, contacts, tasks, notes, and phone messages. The GroupWise Mobility Service is fast, reliable and scalable, and supports the latest device operating systems.

The GroupWise Mobility Service, the GroupWise Sync Agent, and the Device Sync Agent are installed together on a Linux server. A small Mobility system can consist of a single Mobility server. A large Mobility system can consist of multiple Mobility servers.

- "Mobility Server Configuration" on page 7
- "Single Mobility Server System" on page 8
- "Multiple Mobility Server System" on page 8
- "Synchronization Capabilities" on page 9

Mobility Server Configuration

The Mobility server must be able to communicate with other servers in your network, and with mobile devices outside your firewall.



Component	Required Configuration
Sync Agents	The Mobility server has one instance of each sync agent. The GroupWise Sync Agent communicates with the GroupWise POA to obtain items from users' mailboxes. The Device Sync Agent transfers GroupWise mailbox items to and from users' mobile devices.
Mobility Admin Console	The web-based Mobility Admin console communicates with the Mobility Service to enable you to configure the sync agents and monitor your Mobility system.

Component	Required Configuration
User Source	You can add users to your Mobility system from an LDAP server or from a GroupWise system. If you use LDAP as your user source, you access the Mobility Admin console as an LDAP user. If you use GroupWise as your user source, you access the Mobility Admin console as the `root` user of the server where the Mobility Service is installed.
GroupWise POA	The Mobility Service must be able to communicate with one GroupWise POA during installation. That POA, as well as additional POAs where mobile device users' mailboxes are located, must be configured to support SOAP communication. The initial POA uses the native GroupWise redirection process to inform the GroupWise Sync Agent how to communicate with the additional POAs throughout your GroupWise system. Thereafter, the GroupWise Sync Agent communicates directly with each POA where mobile device users' mailboxes are located. **IMPORTANT:** A Mobility server can be configured to communicate with one GroupWise system. If you have multiple GroupWise systems, you must set up a Mobility server for each GroupWise system.

Single Mobility Server System

A Mobility system with a single Mobility server can meet the synchronization needs of approximately 750 users with up to 1000 devices. For more detailed scalability information, see "Recommended Number of Devices" on page 14.

Multiple Mobility Server System

You might need to set up a Mobility system that includes multiple Mobility servers to support the following situations:

- **Number of Devices:** You need to support synchronization for more than 750 users with up to 1000 devices.

  Setting up multiple Mobility servers in virtual machines can be a convenient way to support a large number of devices.
- **Location of Users:** You need to support users that are located in distant geographical locations where synchronization performance could be adversely affected by the network connections between users and a remote Mobility server.
- **Location of Synchronized Applications:** GroupWise has meaningful organizational segments (domains and post offices). Having a Mobility server associated with each post office helps balance the synchronization load across all GroupWise users.
- **Quality of Service:** Certain segments of your user population, such as executives of your organization, might expect and require a higher level of synchronization performance than other users. This higher quality of service can be accomplished by setting up a Mobility server specifically for such high-profile users.
- **Address Book Visibility:** The GroupWise Address Book is displayed on mobile devices from the point of view of a specific GroupWise user. As an example, you might have a group of mobile device users who need access to Address Book information about upper-level management in your company and another group of mobile device users who should not have this Address Book information. To meet such needs, you would set up two Mobility servers, one with Address Book visibility that includes upper-level management, and a second one where such Address Book visibility is not provided.

Synchronization Capabilities

The following GroupWise item types can be synchronized to and from mobile devices:

- Email
- Appointments
- Tasks
- Notes
- Address books
- Contacts
- Phone messages
- Folders

As time passes, the following events can affect existing items, and the resulting changes in the items are also synchronized:

Items	Actions That Synchronize
Emails	◆ Send/receive messages ◆ Forward/reply to messages ◆ Mark messages read/unread ◆ Delete messages
Calendar Items	◆ Send/receive appointments ◆ Accept/decline appointments ◆ Modify appointments ◆ Post reminder notes
Tasks	◆ Send/receive/post tasks ◆ Accept/decline tasks ◆ Mark tasks completed ◆ Receive notifications of task completion ◆ Change the due date and priority for posted tasks ◆ Delete tasks
Contacts	◆ Add new contacts ◆ Delete contacts ◆ Modify contact information, including all contact fields and photos
Phone Messages	◆ Receive phone messages ◆ Delete phone messages
Folders	◆ Add/delete folders ◆ Select/deselect folders for synchronization
Attachments	◆ Forward full attachments even when the attachment size limit has been exceeded (on mobile devices that support Smart Forward functionality)

2 GroupWise Mobility Service System Requirements

Before you install the GroupWise Mobility Service, ensure that the Mobility server meets the following system requirements:

- "Mobility Server Requirements" on page 11
- "Directory Requirements" on page 12
- "Web Browser Requirements for the Mobility Admin Console" on page 12
- "GroupWise Requirements" on page 12
- "Mobile Device Requirements" on page 13
- "Recommended Number of Devices" on page 14

Mobility Server Requirements

This section lists the minimum requirements for GroupWise Mobility Service. To see the recommended requirements for one server supporting approximately 750 users and 1000 devices, see "Recommended Number of Devices" on page 14.

- Hardware requirements for the Mobility server:
  - x86-64 processor
  - 2.2 GHz processor; multi-processor system recommended
  - Static IP address
  - Adequate server memory depending on the number of devices supported by the Mobility server
    - 4 GB RAM to support approximately 300 devices
    - 8 GB RAM to support up to the maximum of 750 users with up to 1000 devices
  - 45 MB of disk space for the Mobility Service software
  - 200 GB of disk space recommended for data storage during system operation

    Data storage disk space varies widely depending on the amount of data being synchronized, the number of devices participating in synchronization, the logging level for Mobility Service log files, and other variables specific to your Mobility system implementation.

    The largest consumers of disk space are the Mobility database (`/var/lib/pgsql`) and Mobility Service log files (`/var/log/datasync`). You might want to configure the Mobility server so that `/var` is on a separate partition to allow for convenient expansion.

    Another large consumer of disk space is attachment storage in the `/var/lib/datasync/syncengine/attachments` directory.

    NOTE: The 200 GB recommendation is appropriate for a Mobility server with a heavy load supporting approximately 750 users with up to 1000 devices. A Mobility server supporting substantially fewer devices requires substantially less disk space.

- SLES 12 plus the latest support pack
- PostgreSQL

  If PostgreSQL is not already installed on the Mobility server, the Mobility Service Installation program installs it for you.
- Time synchronization

  For the most reliable synchronization of time-sensitive items, such as appointments, the Mobility server and GroupWise servers should have their time synchronized as closely as possible. This is especially important on virtual machines.

  In order for you to log in to the Mobility Admin console, your workstation and the Mobility server should have their time synchronized.

Directory Requirements

The GroupWise Mobility Service obtains users and groups from an LDAP directory or a GroupWise system.

- Lightweight Directory Access Protocol (LDAP) v3

  Any shipping version of Micro Focus eDirectory fills this requirement. The GroupWise 18 LDAP server also fills this requirement.

  or
- GroupWise 18

  See “GroupWise Requirements” on page 12 for complete details.

Web Browser Requirements for the Mobility Admin Console

Any of the following web browsers:

- Mozilla Firefox 20 or later
- Microsoft Internet Explorer 10 or later
- Safari 6 or later
- Google Chrome 35 or later

GroupWise Requirements

In order for Mobility to interact successfully with a GroupWise POA, your GroupWise system must meet the following requirements:

- GroupWise 18 maintenance must be current. For more information, see Licensing in the *GroupWise 18 Administration Guide*.
- GroupWise 18 or later domain.

  For best synchronization performance, the latest version of GroupWise is strongly recommended.

NOTE: While GroupWise 18 domains are required, your POAs do not have to be updated to 18 to work with Mobility 18.

- You must have at least a basic GroupWise system (one domain and one post office) set up and running. For more information, see GroupWise System Creation in the *GroupWise 18 Installation Guide*.
- The GroupWise Post Office Agent (POA) that the GroupWise Sync Agent communicates with must have SOAP enabled.

  The POA must also be configured with an HTTP user name and password on the Agent Settings property page of the POA object in the GroupWise Admin console (or in ConsoleOne in older GroupWise systems). This enables you to monitor SOAP threads in the POA web console.

  The initial POA uses the native GroupWise redirection process to inform the GroupWise Sync Agent how to communicate with the additional POAs throughout your GroupWise system. Thereafter, the GroupWise Sync Agent communicates directly with each POA where mobile device users' mailboxes are located.

IMPORTANT: All POAs that have Mobility users must have the same SSL setting--ether all enabled for SSL or all disabled for SSL. If you need to check the SSL settings of your POAs, use the SSL Check option in MCheck.

- A GroupWise trusted application key is required so that the GroupWise Sync Agent can authenticate to GroupWise mailboxes without needing GroupWise users' mailbox passwords. For more information, see Creating a Trusted Application and Key in the *GroupWise 18 Administration Guide*.
- A Mobility server can be configured to communicate with one GroupWise system. If you have multiple GroupWise systems, you must set up a Mobility server for each GroupWise system.

Mobile Device Requirements

The Device Sync Agent communicates with mobile devices by using the Microsoft ActiveSync protocol version 16.*x*.

If a mobile device uses an earlier version of ActiveSync, the device can still successfully communicate with the Device Sync Agent, but functionality specific to 16.*x* is not available. If a mobile device uses a later version of ActiveSync, the device can still successfully communicate with the Device Sync Agent, because later versions of ActiveSync are backward compatible with version 16.*x*.

Supported mobile device operating systems include:

- Android 3.*x*, 4.*x*, 5.*x* and 6.*x*
- Apple iOS 5.*x*, 6.x, 7.x, 8.x, 9.x, 10.x, and 11.x
- Windows Phone 7
- Windows 8 and 10 (Phone, Tablet, and Desktop)
- BlackBerry 10.**x**

A user can synchronize data to multiple mobile devices as needed.

For the latest information about supported mobile devices, see the GroupWise Mobility Service Devices Wiki (http://wiki.novell.com/index.php/GroupWise_Mobility_Devices).

Mobile devices communicate directly with the Device Sync Agent to synchronize data. Some mobile devices require a data plan to accomplish this. Others work successfully with a Wi-Fi connection. Some mobile devices can be configured to use either method. Your mobile device carrier is not involved in the synchronization process.

NOTE: The Device Sync Agent does not work with POP, IMAP, SMTP, or other message transfer protocols.

Recommended Number of Devices

The following are the recommended requirements for a single Mobility server. For the minimum requirements, see "Mobility Server Requirements" on page 11.

A single Mobility server can comfortably support approximately 750 users with up to 1000 devices. The following variables were taken into consideration for this configuration:

- Server configuration
- System configuration
- Level of user activity, both in GroupWise and on their mobile devices

Server Configuration

- Virtual machine
- 2.8 GHz processor
- 4 CPUs
- 8 GB RAM

Mobility System Configuration

- 750 users
- 1000 devices

User/Device Traffic

- Average of 181 GroupWise events per minute
  - Email send / read / move to folder / delete
  - Appointment send / accept / decline / delete
  - Folder create
- Average of 474 events per user in a 24-hour period
- Average of 165 device requests per minute
  - Email send / read
- Average of 427 emails from devices in a 24-hour period
- Average of 2479 KB per minute of attachment data transfer
  - 97% under 1 MB
  - 2% between 1 MB and 2 MB
  - 1% above 2 MB

NOTE: You can observe some of these statistics for your own Mobility system using the Dashboard in the Mobility Admin console. For more information, see "Using the Mobility Dashboard" in the *GroupWise Mobility Service 18 Administration Guide*.

Device Profile

- 60% Apple devices
- 37% Android devices
- 10% Windows Mobile devices
- 3% Other

Hardware Performance for Four Days

- 24% average CPU usage
- 17% average disk busy usage
- 26% average memory usage, with 32% maximum and 24% minimum

3 GroupWise Mobility Service Installation

The GroupWise Mobility Service Installation program available in YaST helps you install the Mobility Service software. Then you use the Mobility Administration console to set up your Mobility system.

- "Planning a Mobility System" on page 17
- "Preparing to Install the Mobility Service" on page 26
- "Installing the Mobility Service" on page 28
- "Adding Users to Your Initial Mobility System" on page 32
- "Testing Your Initial Mobility System" on page 33
- "Integrating with Mobile Device Management Applications" on page 35
- "What's Next" on page 37
- "GroupWise Mobility Service Installation Worksheet" on page 38

Planning a Mobility System

You can use the "GroupWise Mobility Service Installation Worksheet" on page 38 to gather the information you need, so that you are prepared to provide the information requested by the Mobility Service Installation program.

The topics in this section present the required information in a convenient planning sequence. The Installation Worksheet organizes the information in the order in which you need it during the installation process.

Planning the Configuration of Your Mobility System

A Mobility system can consist of a single Mobility server or multiple Mobility servers. For planning guidelines, review the following sections as needed:

- "Single Mobility Server System" on page 8
- "Multiple Mobility Server System" on page 8
- "Recommended Number of Devices" on page 14

MOBILITY SERVICE INSTALLATION WORKSHEET

Print one copy of the GroupWise Mobility Service Installation Worksheet for each Mobility server that you are planning for your Mobility system.

If you plan to install the Mobility Service on multiple servers, you can proceed through the planning sections server by server, or you can apply each planning section to all planned servers, and then proceed to the next planning section.

IMPORTANT: For best security, plan to install the Mobility Service software on servers inside your DMZ.

Selecting Mobility Servers

Each server where you install the Mobility Service must meet the system requirements listed in Chapter 2, "GroupWise Mobility Service System Requirements," on page 11. The Mobility Service requires a static IP address.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **Mobility Service Server Information**, specify the IP address or DNS hostname of the server where you plan to install the Mobility Service software.

Selecting the User Source for Your Mobility System

The GroupWise Mobility Service can obtain information about users and groups of users from an LDAP directory such as Micro Focus eDirectory or from a GroupWise system.

If you use LDAP as your user source, you can do the following:

- Use your LDAP management tool to manage the users and groups that are added to your Mobility system.
- Create LDAP groups of users for use in your Mobility system that are not addressable by GroupWise users.
- You can also use the GroupWise 18 LDAP server to provision and manage users. For information about GroupWise LDAP, see Configuring the LDAP Server Capabilities in the *GroupWise 18 Administration Guide*. If you decide to use GroupWise LDAP, you must use GroupWise authentication.

If you use GroupWise as your user source, you can do the following:

- Use the GroupWise Admin console (or ConsoleOne in older GroupWise systems) to manage the users and GroupWise groups (distribution lists in older GroupWise systems) that are added to your Mobility system.

  This keeps user management in a single location for both your GroupWise system and your Mobility system.
- Configure the GroupWise groups (distribution lists in older GroupWise systems) that are specifically for use in your Mobility system with no visibility, so that they are not easily addressable for GroupWise users.

  For more information, see Controlling Object Visibility in the *GroupWise 18 Administration Guide*.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **User Source**, mark whether you want to use LDAP or GroupWise as the source for users and groups of users.

If you plan to use your GroupWise system, skip to "Gathering GroupWise System Information" on page 21.

Gathering LDAP Information (Optional)

If you plan to use LDAP or GroupWise LDAP as your user source, the Mobility Service Installation program needs access to an LDAP directory. The LDAP information that you provide during installation provides you with access to the Mobility Admin console. It also configures the Mobility Admin console for the initial set of LDAP containers where users and groups are located.

- "LDAP Server Network Information" on page 19
- "LDAP Directory Credentials" on page 19
- "LDAP User and Group Containers" on page 20

LDAP Server Network Information

In order to communicate with your LDAP directory, the Mobility Service Installation program needs the IP address or DNS hostname of your LDAP server. It also needs the port number that the LDAP server listens on. The LDAP port number depends on whether the LDAP server requires a secure SSL connection. The default secure port number is 636. The default non-secure LDAP port number is 389.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **LDAP Information**, specify the IP address or DNS hostname of your LDAP server, and mark whether a secure SSL connection is required. If using GroupWise LDAP, a secure connection is required.

If the LDAP server requires a secure connection, additional setup might be required. See "Securing Communication with the LDAP Server" in the *GroupWise Mobility Service 18 Administration Guide*.

IMPORTANT: If there is a firewall between the Mobility server and the LDAP server, be sure to configure the firewall to allow communication on the selected LDAP port (636 or 389).

LDAP Directory Credentials

Depending on the type of LDAP you are planning on using, follow the section below and enter it into the worksheet as follows:

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **LDAP Information**, specify a fully qualified user name with sufficient rights to read the user and group information in your LDAP directory, along with the password for that user.

- "LDAP" on page 19
- "GroupWise LDAP" on page 20

LDAP

In order to access the LDAP directory, the Mobility Service Installation program needs the user name and password of an administrator user in the LDAP directory who has sufficient rights to access the user and group information stored there. At least Read rights are required. You can use the `admin`

LDAP user or an admin-equivalent user. For more information about the required rights for the user you choose, see TID 7006841, “Rights Needed by the LDAP Administrator for the GroupWise Mobility Service” in the Novell Support Knowledgebase (http://www.novell.com/support).

Provide the user name, along with its context in your LDAP directory tree, in the following format:

```
cn=user_name,ou=organizational_unit,o=organization
```

GroupWise LDAP

If you are using GroupWise LDAP for your LDAP source, you need to create an admin app user for Mobility using the GroupWise Admin service. To create the admin app user, run the following curl command on your GroupWise primary domain server:

```
curl -k --user gw_sys_admin:admin_password -X POST -H "Content-Type:application/
json" --data
"{\"name\":\"admin_app\",\"password\":\"admin_app_password\",\"description\":\"app
_description\"}" https://GW_domain_ip:9710/gwadmin-service/system/adminapps
```

The following items need to be replaced in the curl command:

- **gw_sys_admin:** Specify your GroupWise system admin username.
- **admin_password:** Specify the password of your GroupWise system admin.
- **admin_app:** Specify a name for your admin app.
- **admin_app_password:** Specify a password for your admin app.
- **app_description:** Specify the purpose of the admin app. In this case it is for GMS.
- **GW_domain_ip:** Specify the IP address of your GroupWise primary domain server.

NOTE: If you are running this command on a Windows server, curl may not be available. You can download curl from here if needed.

The admin app is then used to authenticate to GroupWise LDAP. You need the admin app name and password. The name of the admin app needs to be specified in Mobility as follows:

```
cn=admin_app_user
```

LDAP User and Group Containers

During installation, the Mobility Service Installation program configures the Mobility Admin console to search for users and groups in specified containers where you, as the LDAP administrator user, have rights to read the user and group information. The Installation program lets you browse for the user and group containers. It then displays the containers in the following LDAP format:

```
ou=container_name,ou=organizational_unit,o=organization
```

Initially, you can add users and groups to your Mobility system from those containers.

If you are using GroupWise LDAP, the base directory will be your GroupWise System Name which can be found in the GroupWise Admin console > **System** > **Information**. It is listed at the top of the pop up window as **Information - *system_name***. Using that, the base directory should be specified as follows:

```
o=system_name
```

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **LDAP Containers**, specify a container object and its context in the LDAP directory tree where User objects are located. If Group objects are located in a different container, list that container as well.

After installation, when the Mobility Admin console generates lists of users and groups, it searches the containers you specify, as well as subcontainers. If you want the Mobility Admin console to be able to search multiple and organizationally separate containers for users and groups, you can configure this functionality in the Mobility Admin console. For setup information, see "Searching Multiple LDAP Contexts for Users and Groups" in the *GroupWise Mobility Service 18 Administration Guide*.

Gathering GroupWise System Information

In order to configure the GroupWise Sync Agent as you run the Mobility Service Installation program, you need to gather certain information about the GroupWise system where users want to synchronize data to mobile devices.

- "GroupWise Administration Agent" on page 21
- "GroupWise Trusted Application" on page 21
- "GroupWise Post Office Agent SOAP URL" on page 22
- "GroupWise Address Book User" on page 23

GroupWise Administration Agent

The GroupWise Administration Agent is used to connect to the primary domain of the GroupWise system. You need to know the DNS name of the primary domain server, the port the admin service uses, and the credentials of a user that has admin privileges in GroupWise.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **GroupWise Administration Agent**, specify the DNS name of the primary domain server, the admin service port, and the admin user credentials.

GroupWise Trusted Application

A GroupWise trusted application can log in to a GroupWise Post Office Agent (POA) in order to access GroupWise mailboxes without needing personal user passwords. The GroupWise Sync Agent requires such mailbox access in order to synchronize GroupWise data with mobile devices. In addition, the Device Sync Agent uses trusted application ion through the GroupWise Sync Agent in order to access the GroupWise Address Book. This provides contact lookup beyond the contacts that are downloaded to users' devices from personal address books.

Before you install the Mobility Service, you must set up the GroupWise Sync Agent as a GroupWise trusted application. You might name the trusted application `MobilityService` or `GroupWiseSyncAgent`.

A trusted application uses a key that consists of a long string of letters and numbers to provide ion for the GroupWise POA. The key file is initially created in a location that is accessible to GroupWise. You must transfer the key file to a location that is accessible to the Mobility Service Installation program.

When you set up the GroupWise Sync Agent as a trusted application, you must fill in *only* these three fields in the New Trusted App Key dialog box in the GroupWise Admin console (or in the Create Trusted Application dialog box in ConsoleOne in older GroupWise systems):

- **Name**
- **Location for Key File**
- **Name of Key File**

IMPORTANT: Do not fill in any other fields.

For more information, see Creating a Trusted Application and Key in the *GroupWise 18 Administration Guide*.

Copy the key file to a convenient location on the Mobility server. The Installation program automatically transfers the trusted application key from the key file into the configuration of the GroupWise Sync Agent.

IMPORTANT: Do not use an existing trusted application key that is already in use by another application.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **GroupWise Trusted Application**, specify the name of the trusted application that you created and the location where the Mobility Service Installation program can access the trusted application key file.

You need to create only one trusted application key for the GroupWise Sync Agent, regardless of the number of servers where you install the Mobility Service, and regardless of the number of domains and post offices in your GroupWise system.

NOTE: If your GroupWise system connects to any external GroupWise domains, the external GroupWise system needs its own Mobility Service installation on an additional Mobility server, along with its own separate trusted application key.

GroupWise Post Office Agent SOAP URL

The GroupWise Sync Agent accesses your GroupWise system by communicating with a Post Office Agent (POA). The selected POA must be configured for SOAP.

The Mobility Service Installation program and the GroupWise Sync Agent need the IP address or DNS hostname of the server where the POA is running. In addition, they need the POA SOAP port. The default POA SOAP port is 7191.

Typically, the same port number is used regardless of whether the POA is configured for a secure SSL SOAP connection. The Mobility Service Installation program and the GroupWise Sync Agent need to know whether the connection is secure because they use one of the following URLs to communicate with the POA:

Non-Secure SOAP URL:	`http://`*poa_server_address*`:`*soap_port*`/soap`
Secure SOAP URL:	`https://`*poa_server_address*`:`*soap_port*`/soap`

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **GroupWise Post Office Agent**, specify the IP address or DNS hostname of the server where a POA configured for SOAP is running. Specify the SOAP port, and whether or not the POA requires a secure SSL SOAP connection.

IMPORTANT: By default, the POA communicates with the GroupWise Sync Agent using port 4500 on the Mobility server. If there is a firewall between the Mobility server and the POA server, be sure to configure the firewall on the Mobility server to allow communication on port 4500 from the POA server. If necessary, you can configure the GroupWise Sync Agent to listen on a different port number after installation. For setup information, see "Changing the GroupWise Sync Agent Listening Port" in the *GroupWise Mobility Service 18 Administration Guide*.

GroupWise Address Book User

The Device Sync Agent needs to be able to access the GroupWise Address Book to obtain user information. The Device Sync Agent establishes this access through the GroupWise Sync Agent.

The Device Sync Agent needs Address Book access that is equivalent to a typical user. You control what users see in the GroupWise Address Book by controlling object visibility. You want the Device Sync Agent to access the GroupWise Address Book with the same visibility that a typical GroupWise user has when viewing the GroupWise Address Book. For more information, see Controlling Object Visibility in the *GroupWise 18 Administration Guide*.

You need to select a user whose view of the GroupWise Address Book matches what you want the Device Sync Agent to be able to access. You do not need to provide the password for the GroupWise user because the Device Sync Agent accesses the GroupWise Address Book through the GroupWise Sync Agent, which has trusted application status.

As an example, you might have a group of mobile device users who need access to Address Book information about upper-level management in your company and another group of mobile device users who should not have this Address Book information. To meet such needs, you would set up two Mobility servers, one with Address Book visibility that includes upper-level management, and a second one where such Address Book visibility is not provided. You would achieve this by setting up each Mobility server with an Address Book user whose Address Book visibility provides the visibility appropriate for all users on that Mobility server.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **GroupWise Address Book User**, specify a valid GroupWise user name that the Device Sync Agent can use to access the GroupWise Address Book to obtain contact information.

Gathering Mobile Device Information

The Device Sync Agent needs certain configuration information about the mobile devices that it synchronizes GroupWise data with.

- "Device Connection Port" on page 24
- "Server Certificate" on page 24

For device-specific information, see the GroupWise Mobility Service Devices Wiki (http://wiki.novell.com/index.php/GroupWise_Mobility_Devices).

Device Connection Port

By default, the Device Sync Agent uses all available IP addresses on the Mobility server. You can bind the Device Sync Agent to a specific IP address after installation. For setup information, see "Binding to a Specific IP Address" in the *GroupWise Mobility Service 18 Administration Guide*.

Typically, the Device Sync Agent uses port 443 for secure SSL HTTP connections with mobile devices and port 80 for non-secure HTTP connections. If mobile devices connect directly to the Device Sync Agent, a secure HTTP connection is strongly recommended. If mobile devices connect to the Device Sync Agent through a security application such as Micro Focus Access Manager or Micro Focus ZENworks Mobile Management, the Device Sync Agent can appropriately be configured with a non-secure HTTP connection. For more information, see "Integrating with Mobile Device Management Applications" on page 35.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **Device Connection Port**, mark whether you want to configure the Device Sync Agent to use a secure or non-secure HTTP port to communicate with mobile devices. Specify the port number used by the mobile devices that your Mobility system supports.

IMPORTANT: If there is a firewall between the Mobility server and users' mobile devices, be sure to configure the firewall to allow communication on the selected HTTP port (443 or 80).

Server Certificate

In order to use a secure SSL HTTP connection between the Device Sync Agent and mobile devices, a server certificate is required. If you do not already have a certificate signed by a certificate authority (CA) for the Mobility server, the Mobility Service Installation program can generate a self-signed certificate for you. However, you should obtain a commercially signed certificate as soon after installation as possible.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **Mobile Device Port**, mark whether you want the Mobility Service Installation program to generate a self-signed certificate for you. If you already have a commercially signed certificate, specify the location of the certificate file. Ensure that the location is accessible to the Mobility Service Installation program on the Mobility server.

For more information about certificates, see "Securing Communication between the Device Sync Agent and Mobile Devices" in the *GroupWise Mobility Service 18 Administration Guide*.

Planning the Mobility Database

When you run the Mobility Service Installation program, it creates a PostgreSQL database that is used to store the Mobility system configuration information that you see in the Mobility Admin console. It also stores pending events when synchronization is interrupted.

The Mobility Service database is named `datasync`, and the user that has access is named `datasync_user`. You must supply the password for the Mobility Service database user.

IMPORTANT: Choose the password carefully, because you cannot change it. Do not use an asterisk (*) or a semi-colon (;) in the password.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **Mobility Database**, specify the password that you want to use for the Mobility Service database.

Establishing Mobility System Security

Configuration and administration of your Mobility system is performed through the Mobility Administration console. From the Mobility Admin console, you can do the following:

- Add users, groups of users, and resources to your Mobility system
- Configure and monitor the sync agents
- Reconfigure the connection to your LDAP server if you are using LDAP as your user source
- Configure integration with other applications such as ZENworks Mobile Management and KeyShield SSO

To protect your Mobility system operation and configuration, the Mobility Admin console is protected by a user name and password.

If you are using LDAP as your user source, you must choose one LDAP administrator user to access the Mobility Admin console. This LDAP user becomes the initial Mobility administrator. For simplest administration, use the LDAP Admin user or an admin-equivalent user. However, if you prefer to establish a Mobility administrator user with fewer rights than the LDAP Admin user, ensure that the user has sufficient rights to read the User and Group objects that you need to access as you add users to your Mobility system in the Mobility Admin console. Ensure that you know the LDAP administrator user's password.

If you are using GroupWise as your user source, you log in to the Mobility Admin console by using the `root` user name and password.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **LDAP Information**, specify the LDAP administrator user name and password that you want to grant access to the Mobility Admin console, if you are using LDAP as your user source.

Under **root Access to Mobility Admin Console**, specify the `root` password on the Mobility server. If you are using LDAP, you can use the `root` user and password to access the Mobility Admin console if the LDAP server is down.

If you are using LDAP as your user source, you can add more users as Mobility administrators after installation. For more information, see "Setting Up Multiple Mobility Administrator Users" in the *GroupWise Mobility Service 18 Administration Guide*.

Preparing to Install the Mobility Service

The Mobility Service Installation program cannot run successfully unless you have properly prepared the environment where you run it.

- “Preparing the Linux Server” on page 26
- “Opening Required Ports” on page 27
- “Verifying GroupWise System Availability” on page 27
- “Verifying Certificate Availability” on page 28

Preparing the Linux Server

1. Ensure that the Linux server where you plan to install the Mobility Service meets the system requirements listed in Chapter 2, “GroupWise Mobility Service System Requirements,” on page 11.
2. Ensure that the Mobility server has a static IP address.
3. Ensure that the Mobility server has a valid hostname.

   You can check this using the following command:

   ```
   hostname -f
   ```

   If your SLES server is properly configured, this command returns the hostname of the server.

   If you need to configure the server with a hostname:

   3a In YaST, click **Network Devices > Network Settings**.

   3b Click the **Hostname/DNS** tab.

   3c In the **Hostname** field, specify the hostname of the Mobility server, then click **OK**.

   3d Exit YaST.

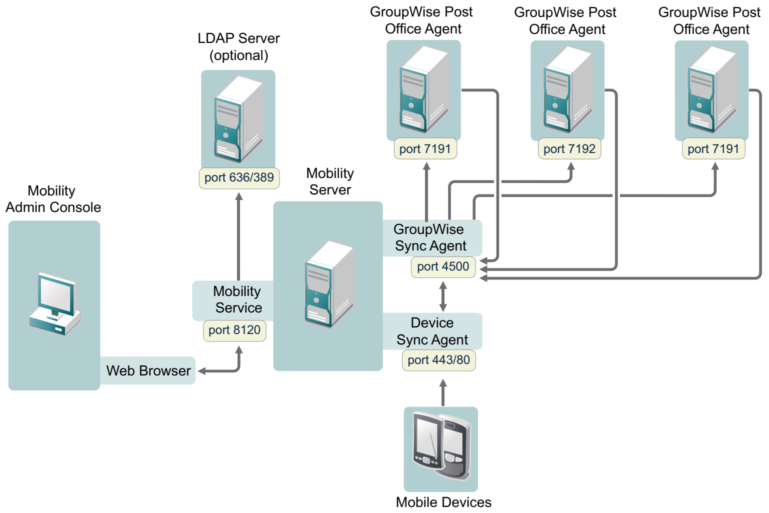
   3e Repeat the `hostname -f` command to verify the hostname.
4. Ensure that the Linux operating system media is available.

   The Mobility Service Installation program might need to install additional operating system RPMs that are required by the Mobility Service. The Mobility Service Installation program can access the operating system files on a DVD or in a repository that is available from an FTP site or a web server.
5. Continue with Opening Required Ports.

Opening Required Ports

1 Ensure that any firewalls between the Mobility server and other applications have been configured to allow communication on the following ports:

Port Number	On Server	Description
636/389	LDAP	LDAP server secure or non-secure port if you are using LDAP as your user source
7191	POA	GroupWise Post Office Agent (POA) SOAP port
4500	Mobility	GroupWise Sync Agent listening port for event notifications
443/80	Mobility	Mobile device secure or non-secure port
8120	Mobility	Mobility Admin console port



The GroupWise Sync Agent initially communicates with the POA that you specify during Mobility Service installation on the SOAP port that you specify. As users connect their mobile devices, the GroupWise Sync Agent determines from the initial POA the IP addresses and port numbers of all POAs where mobile device users have their mailboxes. Therefore, the GroupWise Sync Agent can communicate with multiple POAs throughout your GroupWise system.

2 Continue with Verifying GroupWise System Availability.

Verifying GroupWise System Availability

1 Ensure that the GroupWise trusted application key for the GroupWise Sync Agent is accessible to the Mobility Service Installation program on the Mobility server.

For more information, see Creating a Trusted Application and Key in the *GroupWise 18 Administration Guide*.

2 Ensure that the GroupWise POA that the GroupWise Sync Agent will communicate with is configured for SOAP.

3 Ensure that the GroupWise POA is currently running.

4 Continue with Verifying Certificate Availability.

Verifying Certificate Availability

1 (Conditional) If you have a signed certificate from a certificate authority (CA) as required for configuring secure HTTP connections with mobile devices:

   1a Ensure that the certificate file is accessible to the Mobility Service Installation program on the Mobility server.

   1b (Conditional) If the key file that you received with the certificate included a password, ensure that the password has been removed.

   1c (Conditional) If you received the certificate as multiple files, ensure that you have combined the files into one certificate file.

   For instructions, see "Securing Communication between the Device Sync Agent and Mobile Devices" in the *GroupWise Mobility Service 18 Administration Guide*.

2 (Conditional) If you chose to use YaST to generate a self-signed certificate, ensure that it was created to include the specific DNS hostname of the Mobility server.

3 Continue with Installing the Mobility Service.

For device-specific certificate issues, see GroupWise Mobility Service SSL Issues (http://wiki.novell.com/index.php/Data_Synchronizer_Mobility_Connector_SSL_Issues).

Installing the Mobility Service

Before you run the Mobility Service Installation program, ensure that you have done the following:

❒ Review "Planning a Mobility System" on page 17.

❒ Fill out the GroupWise Mobility Service Installation Worksheet.

If you are setting up a multi-server Mobility system, ensure that you have an Installation Worksheet for each Mobility server. Each Mobility server is independent of other Mobility servers, so you can set them up in whatever order is convenient, based on the overall configuration of your Mobility system.

❒ Complete the tasks in "Preparing to Install the Mobility Service" on page 26.

The following sections step you through the process of installing the Mobility Service and configuring a Mobility system.

- "Obtaining the GroupWise Mobility Service 18 ISO" on page 28
- "Running the Mobility Service Installation Program" on page 29
- "Checking the Status of the Mobility Service" on page 30
- "Using the Mobility Admin Console" on page 30
- "Uninstalling the Mobility Service" on page 31

Obtaining the GroupWise Mobility Service 18 ISO

You can obtain the GroupWise Mobility Service 18 ISO from these locations:

- "Novell Customer Center" on page 29
- "Novell Downloads Website" on page 29

Novell Customer Center

1. Log in to the Novell Customer Center (http://www.novell.com/customercenter).
2. In the **Organization** drop-down list (next to your name in the upper-right corner), select your organization that is entitled to GroupWise Mobility Service.
3. Click **Software**.
4. In the GroupWise section, locate **GroupWise Mobility Service 18**, then click to display the download page.
5. Follow the online instructions to download the GroupWise Mobility Service ISO to a convenient temporary directory on the Mobility server.

   groupwise-mobility-service-*18.0.0*-x86_64-*build_number*.iso

6. Skip to Running the Mobility Service Installation Program.

Novell Downloads Website

1. On Novell Downloads (http://download.novell.com), under **Patches**, click **Search Patches** to display Patch Finder.
2. In the **Select a Product** drop-down list, select **GroupWise**.
3. At the bottom of the GroupWise product list, click **GroupWise Mobility Service 18** to list the available patches.
4. Click **GroupWise Mobility Service 18.0.0**, review the product description, then click **Proceed to Download**.
5. Follow the online instructions to download the GroupWise Mobility Service ISO to a convenient temporary directory on the Mobility server.

   groupwise-mobility-service-*18.0.0*-x86_64-*build_number*.iso

6. Continue with Running the Mobility Service Installation Program.

Running the Mobility Service Installation Program

Mobility is supported on SLES 12. SLES 12 uses an ISO based install.

If you encounter any problems during the installation, check the Mobility Service Installation program log file for information about the problem:

`/var/log/datasync/install.log`

For additional assistance, see Appendix A, "GroupWise Mobility Service Installation Troubleshooting," on page 45.

The Mobility Service Installation program creates the following directories and files:

```
/opt/novell/datasync
/etc/init.d/rcgms
/etc/datasync
/var/lib/datasync
/var/log/datasync
/var/run/datasync
/var/lib/pgsql
```


- "Installing on SLES 12" on page 30

Installing on SLES 12

1. Ensure the SLES 12 iso is available as a repository on the server.
2. Browse to the location where the Mobility Service ISO is located in a terminal and mount the ISO by running the following command:

   ```
   mount -o loop groupwise-mobility-service-18.0.0-x86_64-build_number.iso /mnt
   ```

3. Browse to `/mnt` in the terminal and run the following command to run the install:

   ```
   ./install.sh
   ```

4. Once the files have installed, use the GroupWise Mobility Service Installation Worksheet to configure GroupWise Mobility Service.

Checking the Status of the Mobility Service

The Mobility Service Installation program starts the Mobility Service for you. If the installation proceeded normally, all components of the Mobility Service should be running.

1. In a terminal window on the Mobility server, become `root` by entering `su -` and the root password.
2. Use the following command to check the status of the Mobility Service:

   ```
   rcgms status
   ```

3. Use the following commands to manually start and stop the Mobility Service:

   ```
   rcgms start
   rcgms restart
   rcgms stop
   ```

Using the Mobility Admin Console

The Mobility Service Installation program starts the GroupWise Sync Agent and the Device Sync Agent for you. Use the Mobility Admin console to check sync agent status.

1. In your web browser, access the Mobility Admin console at the following URL:

   ```
   https://mobility_server_address:8120
   ```

Replace *mobility_server_address* with the IP address or DNS hostname of the server where the Mobility Service is installed.

2 Log in as the Mobility administrator (the LDAP Admin user that was set up during installation, or `root`).

   The sync agents should display a status of **Running**.

3 (Conditional) If one or both sync agents are not yet running:

   3a Start the GroupWise Sync Agent first.

   3b Start the Device Sync Agent second.

   The GroupWise Sync Agent accesses the GroupWise Address Book to obtain information needed by the Device Sync Agent.

4 (Conditional) If you encounter problems starting the sync agents, see the following troubleshooting resources:

   - Appendix A, "GroupWise Mobility Service Installation Troubleshooting," on page 45
   - "GroupWise Mobility System Troubleshooting" in the *GroupWise Mobility Service 18 Administration Guide*
   - "Working with Log Files" in the *GroupWise Mobility Service 18 Administration Guide*

5 Skip to "Adding Users to Your Initial Mobility System" on page 32.

Uninstalling the Mobility Service

IMPORTANT: When you uninstall the Mobility Service software, certificate files are also deleted. If you have obtained commercially signed certificates for use in your Mobility system, back them up before you uninstall the Mobility Service software.

1 In a terminal window on the Mobility server, become `root` by entering `su -` and the root password.

2 Change to the following directory:

```
/opt/novell/datasync
```

3 Run the Mobility Uninstallation script:

```
./uninstall.sh
```

The Uninstallation script stops the Mobility Service, the sync agents, and the PostgreSQL database server It also uninstalls all Mobility Service RPMs, drops the Mobility Service PostgreSQL database, and deletes the following directories and files from the Mobility server:

```
/opt/novell/datasync
/etc/init.d/rcgms
/etc/datasync
/var/lib/datasync
/var/log/datasync
/var/run/datasync
/var/lib/pgsql
```

4 Remove the Mobility Service repository from the Linux server.

IMPORTANT: If you do not remove the existing Mobility Service repository, you cannot successfully install the next version of the Mobility Service software.

   4a In YaST, click **Software > Software Repositories**.

   4b Select the Mobility Service repository, then click **Delete**.

5 (Conditional) If you encounter problems reinstalling the Mobility Service after uninstalling it, see "A reinstallation of the Mobility Service software does not proceed normally" on page 47.

Adding Users to Your Initial Mobility System

After you install the Mobility Service, use the Mobility Administration console to add users to your Mobility system. Initially, add a small number of users for testing purposes. The initial users should be active GroupWise users.

1 In your web browser, access the Mobility Admin console at the following URL:

   `https://mobility_server_address:8120`

   Replace *mobility_server_address* with the IP address or DNS hostname of the server where the Mobility Service is installed.

2 Log in as the Mobility administrator (the LDAP Admin user that was set up during installation, or `root`).

3 In the Mobility Admin console, click **Users**, then click **Add Users**.

4 Select the user source (**LDAP** or **GroupWise**).

5 In the **Search** field, type the first or last name of a specific user, then click **Search**.

   or

   Click **Search** to list the users in the user source that the Mobility Admin console has been configured to search.

6 Select one or more users to add to your Mobility system.

7 (Conditional) If you are using LDAP as the user source and if the user's GroupWise user name is not the same as the user's LDAP user name:

   7a In the **Default Name** column, click the user name.

   7b Enter the user's GroupWise user name in the text box.

   The Mobility Service uses default user names to match users who have different user names in GroupWise and in the LDAP directory.

8 Click **Add** to add the users to your Mobility system.

9 After you have tested your Mobility system, add the rest of your mobile device users.

   For instructions, see "GroupWise Mobility User Management" in the *GroupWise Mobility Service 18 Administration Guide*.

10 Continue with Testing Your Initial Mobility System.

Testing Your Initial Mobility System

After you have added a few users to your Mobility system, you can watch the initial synchronization of their devices and send a few test messages.

- "Managing Initial Synchronization of Users" on page 33
- "Helping Mobile Device Users Understand Synchronization" on page 34
- "Testing Synchronization" on page 34

Managing Initial Synchronization of Users

From your point of view as the Mobility administrator, initial synchronization means that GroupWise data has been synchronized from GroupWise to the Mobility System. This means that the data is ready to be synchronized to users' mobile devices as soon as users configure their devices to connect to the Mobility system.

Initial synchronization provides the following synchronization of GroupWise items:

- **Contacts** from all personal address books, excluding the Frequent Contacts address book

  You can change this personal address book selection setting for users after installation in the Mobility Admin console. For instructions, see "Customizing a User's Synchronization Settings" in the *GroupWise Mobility Service 18 Administration Guide*. Users can also change their own synchronization settings on the Mobility Settings page in the Mobility Admin console. For more information, see the GroupWise Mobility Quick Start for Mobile Device Users.

  The GroupWise Address Book cannot be synchronized to mobile devices. However, users can still access individual contacts in the GroupWise Address Book if their mobile devices can do a Global Address List (GAL) lookup. As an alternative, users can create a personal address book that is a subset of the GroupWise Address Book to synchronize to their mobile devices.
- **Calendar items** (appointments and reminder notes) from the last two weeks and all future calendar items

  Shared calendars are synchronized only for the owners of the shared calendars. If shared calendars are very important to users, shared calendar owners can post them to the Internet. For more information, see Publishing Personal Calendars on the Internet in the *GroupWise 18 Client User Guide*.

  After the owner publishes the calendar, other users can view the calendar URL in the web browser on their mobile devices.

  To provide this functionality, at least one Calendar Publishing Host must be set up in the GroupWise system. For more information, see Setting Up the GroupWise Calendar Publishing Host in the *GroupWise 18 Installation Guide*.
- **Email messages** in the Mailbox folder for the last three days

  If users want to receive more existing email messages on their devices, they can configure their mobile devices to request additional existing email messages.
- **Tasks** with due dates in the last two weeks and all future tasks

  Completed and uncompleted tasks are synchronized. Posted and group tasks are synchronized. Tasks that originate as other GroupWise item types (such as emails or calendar items) are synchronized as tasks when they are dragged to the Tasklist, when they are displayed in the Tasklist, or when they are changed to tasks.

  The GroupWise Tasklist does not synchronize to mobile devices. You cannot create a tasklist on a mobile device that is associated with a GroupWise account.

- **Phone messages** for the last three days
- **Folders** in the Cabinet (but not items in folders until users request them by opening folders on their mobile devices)
- **Attachments** if they do not exceed your Mobility system size limits

  If an item has an attachment that does not synchronize, a message notifies the user. For more information, see "Controlling Synchronization Size Limits" in the *GroupWise Mobility Service 18 Administration Guide*.

When you add several users to your Mobility system at the same time, initial synchronization is performed for four users at a time. When it finishes with one of the four users, it starts on another user.

You can monitor the progress of initial synchronization in the Mobility Admin console. For instructions, see "Monitoring User Status" and "Monitoring Device Status" in the *GroupWise Mobility Service 18 Administration Guide*.

IMPORTANT: You should complete initial synchronization before you notify users to configure their mobile devices. Initial synchronization can take a substantial amount of time, depending on the amount of data to synchronize.

Occasionally, initial synchronization fails, and troubleshooting is required. For assistance, see "Device Troubleshooting" in the *GroupWise Mobility Service 18 Administration Guide*.

Helping Mobile Device Users Understand Synchronization

To help your mobile device users get started efficiently, notify them of the following information:

- Users must correctly configure their mobile devices in order to connect to the Mobility system. For instructions, see the GroupWise Mobility Quick Start for Mobile Device Users. Ensure that you provide all the information about your Mobility system that users need in order to successfully configure their devices. To make this process easier, see "Using Autodiscover to Simplify Device Setup" in the *GroupWise Mobility Service 18 Administration Guide*.

  IMPORTANT: Print the GroupWise Mobility Quick Start for Mobile Device Users and distribute it to your mobile device users, or email them the link to it (http://www.novell.com/documentation/groupwisemobility2/pdfdoc/gwmob18_qs_user/gwmob18_qs_user.pdf), to help them configure their devices correctly.

- For device-specific information, see the GroupWise Mobility Service Devices Wiki (http://wiki.novell.com/index.php/GroupWise_Mobility_Devices).

These two sources of information can help eliminate the need for mobile device users to contact you with functional and device-specific questions as they start synchronizing GroupWise data to their mobile devices.

Testing Synchronization

1. Test GroupWise data synchronization by logging in to your GroupWise mailbox and sending yourself an email message.
2. Reply to the message from your mobile device.

   If the message synchronizes to your mobile device and the reply on your mobile device synchronizes back to GroupWise, your basic Mobility system is up and running.

3 (Conditional) If the message does not synchronize successfully, see the following troubleshooting resources:

In this *GroupWise Mobility Service 18 Installation Guide*:

- "GroupWise Mobility Service Installation Troubleshooting" on page 45

In the *GroupWise Mobility Service 18 Administration Guide*:

- "Device Troubleshooting"
- "Mobility Service Troubleshooting"
- "GroupWise Sync Agent Troubleshooting"
- "Device Sync Agent Troubleshooting"

4 To customize and expand your Mobility system, see "What's Next" on page 37.

Integrating with Mobile Device Management Applications

The GroupWise Mobility Service can be used with several mobile device management (MDM) applications:

- "Micro Focus ZENworks Mobile Management" on page 35
- "Other MDM Solutions" on page 37

Micro Focus ZENworks Mobile Management

Micro Focus ZENworks Mobile Management is a mobile device management solution that provides centralized management and control of mobile devices throughout your enterprise network. For complete information, see the ZENworks Mobile Management Documentation website (https://www.novell.com/documentation/zenworksmobile32/).

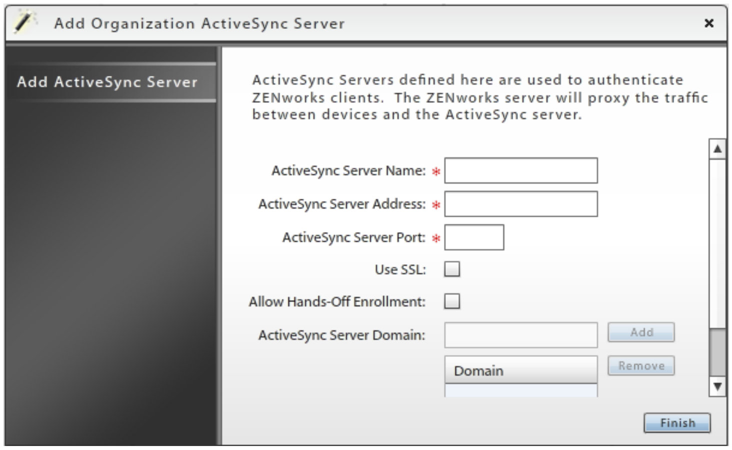
When you configure ZENworks Mobile Management to work with your Mobility system, all of the powerful features of ZENworks Mobile Management are available for managing the mobile devices of your GroupWise users.

1 Configure ZENworks Mobile Management with information about your Mobility server:

1a Log in to the ZENworks Mobile Management Dashboard.

1b Click **Organization** > **Administrative Servers** > **ActiveSync Servers** to list your existing ActiveSync servers.

1c Click **Add ActiveSync Server**.



1d In the **ActiveSync Server Name** field, specify the DNS hostname of your Mobility server, such as `gwmobility`.

1e In the **ActiveSyncServer Address** field, specify the fully qualified hostname of your Mobility server, such as `gwmobility.provo.novell.com`.

1f In the **ActiveSync Server Port** field, specify `443` for a secure connection.

1g Select **Use SSL**.

1h In the **Domain** field, specify the Internet domain where your Mobility server is located, such as `novell.com`, then click **Add**.

1i Click **Finish** to save the information about your Mobility server.

1j (Conditional) If you have multiple Mobility servers, repeat Step 1c through Step 1i, providing information about each Mobility server.

1k (Conditional) If you have multiple ZENworks Mobile Management servers, configure additional servers with information about your Mobility server(s).

2 Ensure that your GroupWise mobile device users have been added to ZENworks Mobile Management.

3 Configure your Mobility system with information about ZENworks Mobile Management:

3a In the Mobility Admin console, click **Config**.

3b On the **General** page, scroll down to the **MDM Server** field.

3c Specify the IP address of the ZENworks Mobile Management server where you provided information about your Mobility server.

3d (Conditional) If you configured multiple ZENworks Mobile Management servers with information about your Mobility server, specify the IP addresses in a comma-delimited list.

3e Click **Save** to save the new setting(s).

3f Restart the Mobility Service:

```
rcgms restart
```

4 View the GroupWise mobile device users that have been added to ZENworks Mobile Management:

4a From the ZENworks Mobile Management Dashboard, click **Users**.

4b Scroll horizontally to view various types of information about GroupWise users and their mobile devices, including the following:

- Time of last synchronization
- Phone number
- Mobile device model
- Mobile device operating system and version

5 Verify that the configuration is successful:

5a In the Mobility Admin console, click **Users**, then click a user who has a device to add.

5b Add the new device through ZENworks Mobile Management.

5c When the device appears on the User/Device Actions page, verify that it has `_zmm` appended to the device ID.

The `_zmm` on the device ID shows that the user connected the device to your Mobility system through ZENworks Mobile Management.

If you require existing mobile device users to re-add their devices through ZENworks Mobile Management, they initially have two device IDs, one with `_zmm` and one without. This prevents ZENworks Mobile Management requests from conflicting with regular device requests. The old device ID disappears from the User/Device Actions page in about a month.

Other MDM Solutions

Because GroupWise Mobility Service 18 supports ActiveSync 16, it can be used with the BlackBerry Enterprise Service 10 device management and security platform, and with any other MDM solution that supports ActiveSync 16. Unless you are using BlackBerry MDM, you should populate the Mobility Admin console > **Config** > **General** > **MDM Server** field with the IP address of your MDM server. If you are using BlackBerry MDM, you do not need to populate this field.

What's Next

- "Managing Your Mobility System" on page 37
- "Managing the GroupWise Sync Agent" on page 38
- "Managing the Device Sync Agent" on page 38

Managing Your Mobility System

After your Mobility system is running smoothly, see the following sections in the *GroupWise Mobility Service 18 Administration Guide* for instructions on maintaining your Mobility system:

- "GroupWise Mobility Administration Console"
- "GroupWise Mobility System Management"
- "GroupWise Sync Agent Configuration"
- "Device Sync Agent Configuration"
- "GroupWise Mobility System Monitoring"

* “GroupWise Mobility User Management”
* “GroupWise Mobility Device Management”
* “GroupWise Mobility System Security”
* “GroupWise Mobility System Troubleshooting”

Managing the GroupWise Sync Agent

After the GroupWise Sync Agent is successfully synchronizing data for the initial set of GroupWise users, see the following sections in the *GroupWise Mobility Service 18 Administration Guide* for instructions on customizing and maintaining the GroupWise Sync Agent:

* “Selecting GroupWise Items to Synchronize”
* “Increasing GroupWise Sync Agent Reliability or Performance”
* “Ignoring Old GroupWise Items”
* “Clearing Accumulated GroupWise Events”
* “Changing the GroupWise Sync Agent Listening Port”
* “Enabling and Disabling SSL for POA SOAP Connections”
* “Matching GroupWise Configuration Changes”
* “Modifying or Preventing Synchronization of Specified Items by Using an XSLT Filter”

Managing the Device Sync Agent

After the Device Sync Agent is successfully synchronizing data for the initial set of mobile device users, see the following sections in the *GroupWise Mobility Service 18 Administration Guide* for instructions on customizing and maintaining the Device Sync Agent:

* “Blocking/Unblocking All Incoming Devices”
* “Enabling a Device Password Security Policy”
* “Quarantining New Devices to Prevent Immediate Connection”
* “Controlling the Maximum Number of Devices per User”
* “Removing Unused Devices Automatically”
* “Controlling the Maximum Number of Devices per User”
* “Binding to a Specific IP Address”
* “Enabling a Device Password Security Policy”
* “Changing the Address Book User”

GroupWise Mobility Service Installation Worksheet

Installation Field	Value for Your Mobility System	For More Information, See
Mobility Server Information ◆ IP address ◆ Hostname		“Selecting Mobility Servers” on page 18.

Installation Field	Value for Your Mobility System	For More Information, See
User Source ◆ GroupWise ◆ LDAP		"Selecting the User Source for Your Mobility System" on page 18

LDAP Information
◆ LDAP server
  ◆ IP address
  ◆ Hostname
◆ Secure LDAP Port?
  ◆ Yes
  Default port: 636
  ◆ No
  Default port: 389
◆ LDAP server credentials
  ◆ LDAP administrator DN
  ◆ LDAP administrator password
◆ LDAP containers
  ◆ Users
  ◆ Groups
◆ Mobility Admin console credentials
  ◆ Admin login DN
  ◆ Admin password
		"Gathering LDAP Information (Optional)" on page 19.
		"Establishing Mobility System Security" on page 25.

Mobility Service Database ◆ Database name: `datasync` ◆ Database user: `datasync_user` ◆ Database password		"Gathering Mobile Device Information" on page 23.
GroupWise Administration Agent ◆ Admin Agent DNS hostname ◆ Admin Agent port Default port: 9710 ◆ User with admin privileges		"GroupWise Administration Agent" on page 21.

Installation Field	Value for Your Mobility System	For More Information, See
GroupWise Trusted Application ◆ Trusted application name ◆ Trusted application key file		"GroupWise Trusted Application" on page 21.
GroupWise Post Office Agent ◆ POA IP address or DNS hostname ◆ POA SOAP port Default port: 7191 ◆ Secure: Yes / No		"GroupWise Post Office Agent SOAP URL" on page 22.
Device Connection Port: ◆ Secure LDAP port: Yes Default port: 443 ◆ Generate self-signed certificate? ◆ Yes ◆ No Certificate file: ◆ Secure LDAP port: No Default port: 80		"Device Connection Port" on page 24 and "Server Certificate" on page 24.
GroupWise Address Book User:		"GroupWise Address Book User" on page 23.
Novell Customer Center Registration: ◆ Register later ◆ Register now ◆ Email address ◆ Activation code		"Establishing Mobility System Security" on page 25.
root Access for Mobility Admin Console ◆ root password		"Establishing Mobility System Security" on page 25

4 GroupWise Mobility Service Update

Updating to GroupWise Mobility Service 18

The update process pertains to either the following types of updates:

- Any version of GroupWise Mobility Service to GroupWise Mobility Service 18.
- Any version of the Novell Data Synchronizer Mobility Pack to GroupWise Mobility Service 18.

Complete the following steps to update to GroupWise Mobility Service 18:

- "Obtaining the GroupWise Mobility Service 18 ISO" on page 41
- "Upgrading GroupWise Mobility Service" on page 42
- "Checking the Status of the Mobility Service after Update" on page 43
- "Changing the User Source for Your Mobility System (Optional)" on page 43

Obtaining the GroupWise Mobility Service 18 ISO

You can obtain the GroupWise Mobility Service 18 ISO from these locations:

- "Novell Customer Center" on page 41
- "Novell Downloads Website" on page 41

Novell Customer Center

1. Log in to the Novell Customer Center (http://www.novell.com/customercenter).
2. In the **Organization** drop-down list (next to your name in the upper-right corner), select your organization that is entitled to GroupWise Mobility Service.
3. Click **Software**.
4. In the GroupWise section, locate **GroupWise Mobility Service 18**, then click to display the download page.
5. Follow the online instructions to download the GroupWise Mobility Service ISO to a convenient temporary directory on the Mobility server.

   `groupwise-mobility-service-`*`18.0.0`*`-x86_64-`*`build_number`*`.iso`

Novell Downloads Website

1. On Novell Downloads (http://download.novell.com), under **Patches**, click **Search Patches** to display Patch Finder.
2. In the **Select a Product** drop-down list, select **GroupWise**.
3. At the bottom of the GroupWise product list, click **GroupWise Mobility Service 18** to list the available patches.
4. Click **GroupWise Mobility Service 18.0.0**, review the product description, then click **Proceed to Download**.

5 Follow the online instructions to download the GroupWise Mobility Service ISO file to a convenient temporary directory on the Mobility server.

groupwise-mobility-service-*18.0.0*-x86_64-*build_number*.iso

Upgrading GroupWise Mobility Service

- "Upgrading Mobility on SLES 12" on page 42
- "Upgrading from SLES 11 to SLES 12" on page 42

Upgrading Mobility on SLES 12

Before upgrading Mobility, the new ISO must be downloaded to the server.

- ❒ In a terminal, mount the GroupWise Mobility ISO using the following command:

  mount -o loop <*path to the Mobility ISO*> /mnt

- ❒ Browse to /mnt and run the install.sh.
- ❒ Follow the prompts to upgrade Mobility.

Upgrading from SLES 11 to SLES 12

Before you can upgrade from SLES 11 to SLES 12, the following prerequisites must be met:

- ❒ The latest GMS 14.2.x must be installed on the SLES 11 server before the upgrade to SLES 12.
- ❒ The SLES 11 server must be registered with NCC.
- ❒ You must be updating to SLES 12 SP1 or SP2. Updating to SLES 12 SP3 or later requires an extra step to be performed from SLES 12 SP2.
- ❒ You must have the GMS 18.0 or later iso to use for the upgrade after upgrading to SLES 12.

To upgrade the server from SLES 11 to SLES 12, do the following:

- ❒ Run /opt/novell/datasync/tools/pgUpdate.sh to update postgresql. This can be done at any time before upgrading the OS.
- ❒ Upgrade the OS to SLES 12 (https://www.suse.com/documentation/sles-12/book_sle_deployment/data/part_update.html).

  NOTE: As part of the upgrade, the Mobility server files may be removed. This does not affect the Mobility data.

- ❒ In a terminal, mount the GroupWise Mobility ISO for SLES 12 using the following command:

  mount -o loop <*path to the Mobility ISO*> /mnt

- ❒ Browse to /mnt and run the install.sh.
- ❒ Follow the prompts to upgrade Mobility.

To upgrade the server from SLES 12 SP2 to SLES 12 SP3, do the following:

- ❒ Run `/opt/novell/datasync/tools/pgUpdate94to96.sh` to update postgresql. This can be done at any time before upgrading the OS.
- ❒ Upgrade the OS to SLES 12 SP3.

Checking the Status of the Mobility Service after Update

The Mobility Service Update script starts the Mobility Service for you. If the update proceeded normally, all components of the Mobility Service should be running.

1. In a terminal window on the Mobility server, become `root` by entering `su -` and the root password.
2. Use the following command to check the status of the Mobility Service:

   ```
   rcgms status
   ```

3. Use the following commands to manually start and stop the Mobility Service:

   ```
   rcgms start
   rcgms restart
   rcgms stop
   ```

Changing the User Source for Your Mobility System (Optional)

For background information about the user source alternatives, see “Selecting the User Source for Your Mobility System” on page 18. For usage instructions, see “Changing between LDAP and GroupWise as the User Source” in the *GroupWise Mobility Service 18 Administration Guide*.

The Data Synchronizer Mobility Pack created a Synchronizer system based on LDAP as the user source for user provisioning and, optionally, for device authentication. In Synchronizer Web Admin, the **Authentication Type** setting on the Mobility Connector Settings page set the device authentication method for your Synchronizer system. This setting automatically transferred to the **Authentication** setting on the User Source page in the Mobility Admin console.

IMPORTANT: If you are comfortable with the configuration that you used for your Synchronizer system, there is no need to change it for your Mobility system.

If you want to start using GroupWise as the user source for provisioning, new mobile device users are added to your Mobility system based on their GroupWise location (*user_name.post_office_domain*). Existing mobile device users are still associated with their LDAP context (cn=*user_name*,ou=*organizational_unit*,org=*organization*). On the Users page, you can determine the source of each user by mousing over it.

There is no direct way to change an existing user from being associated with LDAP to being associated with GroupWise. If it is important for you to do this, you must delete the user as an LDAP user, and then add the user as a GroupWise user. After this occurs, the best practice for data integrity is to have the mobile device user delete and re-add the email account on the device.

There is also no direct way to change from using an LDAP group to using a GroupWise group (distribution list in older GroupWise systems). As with individual users, you must delete the LDAP group from your Mobility system (which deletes all the LDAP users in the LDAP group), and then add the GroupWise group (which adds all the users based on the GroupWise group). Again, the affected users should delete and re-add their email accounts on their devices.

You might want to accomplish this transition over time, a few users at a time. If you want to accomplish the transition all at once, you can create a new Mobility system, based entirely on GroupWise provisioning and ion, and then switch from the old system to the new system, perhaps over night, without notifying your mobile device users. Most users will likely not notice the change. You can then have those users that contact you about data integrity issues delete and re-add their email accounts in order to resynchronize the GroupWise data.

A GroupWise Mobility Service Installation Troubleshooting

- "The GroupWise Mobility Service Installation program does not behave as documented" on page 45
- "The GroupWise Mobility Service Installation program cannot communicate with the LDAP server" on page 45
- "The GroupWise Mobility Service Installation program cannot communicate with the GroupWise POA" on page 46
- "The GroupWise Mobility Service Installation program cannot communicate with any required application" on page 46
- "The Mobility Service does not start" on page 46
- "You cannot access the Mobility Admin console after installation" on page 47
- "A reinstallation of the Mobility Service software does not proceed normally" on page 47

See also the following sections in the *GroupWise Mobility Service 18 Administration Guide*:

- "Device Troubleshooting"
- "GroupWise Sync Agent Troubleshooting"
- "Device Sync Agent Troubleshooting"
- "Working with Log Files"

The GroupWise Mobility Service Installation program does not behave as documented

Possible Cause: You are trying to install the GroupWise Mobility Service on 32-bit hardware.

Action: Install the GroupWise Mobility Service on 64-bit hardware that meets the system requirements described in "Mobility Server Requirements" on page 11.

The GroupWise Mobility Service Installation program cannot communicate with the LDAP server

Possible Cause: A firewall is blocking communication between the Installation program and the LDAP server.

Action: Ensure that communication through the firewall is allowed on port 636 for a secure LDAP connection or port 389 for a non-secure LDAP connection.

Possible Cause: The LDAP server is not functioning correctly.

Action: Restart the LDAP server.

Possible Cause: You specified the LDAP server settings incorrectly.

Action: Double-check the LDAP server settings you entered in the Installation program.

The GroupWise Mobility Service Installation program cannot communicate with the GroupWise POA

Possible Cause: A firewall is blocking communication between the Installation program and the POA server.

Action: Ensure that communication through the firewall is allowed on port 4500.

Possible Cause: The POA is not running.

Action: Start the POA.

Possible Cause: You specified the POA server settings incorrectly.

Action: Double-check the POA server settings you entered in the Installation program.

Possible Cause: There is a problem with the GroupWise trusted application key file.

Action: Re-create the GroupWise trusted application key file. You need to fill in only these three fields in the New Trusted App Key dialog box in the GroupWise Admin console (or in the Create Trusted Application dialog box in ConsoleOne in older GroupWise systems): **Name**, **Location for Key File**, and **Name of Key File**. Do not fill in any other fields.

The GroupWise Mobility Service Installation program cannot communicate with any required application

Possible Cause: The required port number is not open.

Action: Review the list of required port numbers in "Opening Required Ports" on page 27.

Action: Use `telnet` to test whether ports are open.

1. Enter the following command in a terminal window:

   ```
   telnet application_host port_number
   ```

   Replace *application_host* with the IP address or DNS hostname of the server where the application is running.

   Replace *port_number* with the port number on which the Installation program is attempting to communicate with the application.

2. (Conditional) If the terminal windows goes blank, with the cursor in the upper-left corner, enter `quit` to exit the telnet session.

   The port is open. The Installation program should be able to communicate with the application.

3. (Conditional) If a `Connection failed` message displays, open the port through the firewall to enable the Installation program to communicate with the application.

The Mobility Service does not start

Possible Cause: PostgreSQL is not running on the Mobility server.

Action: Check the status of PostgreSQL on the Mobility server, and start it manually if necessary.

```
rcpostgresql status
rcpostgresql start
```

You cannot access the Mobility Admin console after installation

Possible Cause: The date and time on the Mobility server does not match the date and time on the GroupWise server.

Action: Reset the time on the Mobility server to match the time on the GroupWise server. This Mobility system requirement is listed in "Mobility Server Requirements" on page 11.

A reinstallation of the Mobility Service software does not proceed normally

Possible Cause: The previous installation of the Mobility Service software was not completely uninstalled.

Action: The standard uninstallation procedure provided in "Uninstalling the Mobility Service" on page 31 occasionally fails to completely uninstall the GroupWise Mobility Service because of various server-specific issues. When the Mobility Service software is not completely uninstalled, the next installation does not proceed normally. For example, you might encounter problems configuring LDAP access during installation.

1. To ensure that the Mobility Service software has been completely uninstalled, perform the following checks:
   - In YaST, click **Software > Add-On Products**.

     The GroupWise Mobility Service should not be listed. If it is still listed, select it, then click **Delete**.
   - In YaST, click **Software > Software Repositories**.

     The GroupWise Mobility Service repository should not be listed. If it is still listed, select it, then click **Delete**.
   - In YaST, click **Software > Software Management**. In the **Filters** drop-down list, select **Patterns**.

     Under the **Primary Functions** heading, the GroupWise Mobility Service should not be listed. If it is still listed, select it. Review the **Packages** list for any packages that were not successfully uninstalled and uninstall them.
   - In YaST, click **Software > Software Management**. In the **Search** field, specify `datasync`, then click **Search**.

     The **Packages** list should be empty. If any Mobility Service packages are still listed, uninstall them.
   - Log in as `root` in a terminal window, then check for Mobility Service RPMs:

     ```
     rpm -qa | grep datasync
     ```

     If any Mobility Service RPMs are still installed, uninstall them:

     ```
     rpm -e rpm_name.rpm
     ```
   - Ensure that none of the following directories still exist on your server:

```
/opt/novell/datasync
/etc/datasync
/var/lib/datasync
/var/log/datasync
/var/run/datasync
/var/lib/pgsql
```

If any of these directories still exist, delete them.

2. After your performing these checks and making changes as needed, restart the Mobility server.
3. Remove the Mobility certificate from any workstations where you have run the Mobility Admin console.

   For example, in Firefox, click **Tools > Options > Advanced > Encryption > View Certificates**. Select the certificate named `DataSync Web Admin`, then click **Delete**.